System Security

VOLUME VI
SECTION 5

The COD System is a United States Department of Education computer system, which may only be used for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

Table of Contents

Privacy Notice

The COD System is a United States Department of Education computer system, which may only be used for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action.

Warning

If such monitoring reveals possible evidence of criminal activity, monitored records will be provided to law enforcement officials.

If you use this computer system, you must understand that all activities may be monitored and recorded by automated processes and/or by Government personnel. Anyone using this system expressly consents to such monitoring.

This system contains personal information protected under the provisions of the Privacy Act of 1974, 5 U.S.C. §552a - - as amended. Violations of the provisions of the Act may subject the offender to criminal penalties.

COD Web Site Access

Beginning in May 2013, the COD Website will no longer be used to create new users or conduct password maintenance. All COD Website users will be required to register through the Federal Student Aid Participation Management System. All COD Website password maintenance will be done via the current process using the Access and Identity Management System (AIMS) website. Additional information will be available via electronic announcements.

Schools and Third-Party servicers who wish to gain access to the COD Website must first be enrolled for COD online service by a school's or organiztion's Primary Destination Point Administrator (PDPA) via the Student Aid Internet Gateway (SAIG) enrollement website and have an FSA User ID and Password. The number of Primary Destination Point Adminstrator is at the discretion of the institution, although it is strongly recommended that the number is limited.

To be enrolled for the COD Online Service, the user must complete three actions outlined below.

Action 1: Submit SAIG Enrollment Form

The user must first complete a SAIG Enrollment Form. ***Note:*** The SAIG Enrollment form cannot be completed online.

To simplify completing the SAIG Enrollment Form, some questions have been pre-filled. In addition, instructions have been included with the form to assist in completing the required questions. Once you have completed the form and have all of the required signatures, send the completed form to Federal Student Aid as indicated on the signature page instructions.

Once the submitted form is processed, you will receive an e-mail with a pseudo-Social Security Number (SSN) and TG number. Be sure to file these numbers in a secure location; they should not be shared with other individuals. These numbers will also be needed to request and register for an FSA User ID (see the next section below). ***Note:*** Each user associated with multiple schools must enroll for the COD Online Service for ***each school*** for which COD Web site access is needed.

Action 2: Obtain FSA User ID and Password

After the COD Web site user is enrolled for the COD Online Service, he or she can register for an FSA User ID and password. Users who need to register for an FSA User ID and password can do so by completing the following steps:

Step 1: Go to the SAIG Enrollment Web site and click on the "FSA User ID Registration" link on the left-hand side of the home page.

Step 2: Enter the identifying information requested and click on Submit. This will include your pseudo-SSN.

Third Party Vendor Information

Third-Party vendor information is requested for information purposes only, and will help COD provide better customer service. This information DOES NOT authorize third-party servicers or vendors to access your school's data.

School's Destination Point Administrator is authorized to set up additional users at their school ONLY. School's Destination Point Adminstrators should NOT set up/enroll COD online services for third-party servicers and/or vendors used by their institution. Third-Party Servicers are responsible for requesting their own Destination Point Administrator. Due to relationship data stored within COD, third-party servicer web users will be able to view data for the schools that they have a relationship with.

Step 3: Follow the remaining steps, which include establishing a password and setting up challenge questions.
Once the registration process is complete, you will be sent the FSA User ID via e-mail. You will then need to register your TFA token for use with your new FSA User ID.

Action 3: Register TFA Token

After the FSA User ID registration process is complete and the FSA User ID is received, the user will then need to register his or her TFA token to associate it with the FSA User ID. Users who do not have a TFA token should contact their Primary Destination Point Administrator (PDPA) to obtain one. ***Note***: If a user already has a TFA token because he or she accesses another Federal Student Aid system, the user does not need to register it again.

To register a TFA token, use the following steps:

1. Go to the following URL: http://sa.ed.gov/enrole/SAWeb/selfmenu.jsp.
2. Click on the token registration link: "Register/Maintain Token."
3. Enter your FSA User ID and password and click on "Login."
4. Complete the token registration information.
5. When the "Success" message is displayed, your token has been registered.
6.

Once you have completed all three actions, you will be able to access the COD Web site.

Note: **If a school needs additional TFA tokens, the PDPA should send an e-mail to TFA_Communications@ed.gov, and include the school name and OPE ID on the correspondence.** ***Note:*** **Each user associated with multiple schools must enroll for the COD Online Service for *each school* for which COD Web site access is needed.**

Rules of Behavior

Schools are encouraged, but not required, to establish Rules of Behavior as part of their business processes related to the COD System. The Rules of Behavior developed by the United States Department of Education are available for reference. Please note that these rules have been established for Department of Education employees. Your institution's rules may be different, but should cover all the areas covered in this example.

Introduction

A good security posture supports the business purpose of the organization. Rules of behavior are designed to provide a schema for sustaining the business process, minimizing disruption, maintaining the ability to continue customer support, and supporting a planned and orderly restoration of service in an emergency.

Federal Student Aid (FSA), Common Origination and Disbursement (COD), processes and stores a variety of sensitive data that is provided by students, colleges/universities, financial, and Government institutions. This information requires protection from unauthorized access, disclosure, or modification based on confidentiality, integrity, and availability requirements. The "Rules of Behavior" apply to all employees/users (including corporate, Government, Modernization Partner, and Trading Partner) of the FSA/COD computer system and their host applications.

The rules delineate responsibilities and expectations for all individuals supporting the COD programs. Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Depending on the severity of the violation, sanctions may range from a verbal or written warning, removal of system privileges/access for a specific period of time, reassignment to other duties, or termination. Violation of these rules and responsibilities could potentially result in prosecution under local, State, and/or Federal law.

Physical Security

- Keep all badges, access codes, and keys under personal protection.
- Wear your assigned identification security badge at all times while in the office/building.
- Ensure your visitors have signed the visitor's log/are escorted at all times.
- Never allow any individual who does not have proper identification access to the office space.
- Stop and question any individual who does not have proper identification, and contact Security immediately. Seek the support and cooperation of co-workers as appropriate.
- Maintain control over your corporate/Government provided hardware/software to prevent theft, unauthorized use/disclosure,

misuse, denial of service, destruction/alteration of data, and/or violation of Privacy Act restrictions.

- Keep your desk clean to ensure that sensitive and proprietary information does not get hidden in minutia and therefore not properly secured/protected when not in use because it is not visible.

Computer Virus Protection

- Use the approved anti-virus software on your personal computer.
- Avoid booting from the `A:` drive.
- Scan all new diskettes before using or distributing them.
- Write-protect all original vendor-supplied diskettes.
- Back up all data on your workstation and file server regularly.
- Use only authorized and appropriately licensed software.
- Report all incidents of computer viruses to your System Security Officer (SSO) or Manager.
- Do not download, introduce, or use unauthorized software from unknown or unverifiable sources. All users are required to comply with safe computing practices to reduce the risk of damage by any type of computer virus.

Computer System Responsibilities

- Do not make copies of system configuration files (that is, /etc/passwd) for your own use, unauthorized use, or to provide to others for unauthorized use.
- Do not attempt to access any data or programs on the COD system for which you do not have authorization or explicit consent from the owner of the data or program.
- Do not, without specific authorization, read, alter, or delete any other person's computer files or electronic mail (E-mail), even if the operating system of the computer allows you to do so.
- Do not engage in, encourage, or conceal any "hacking" or "cracking," denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any computer system within the COD program.
- Do not purposely engage in any activity with the intent to:
    - Degrade the performance of the system;
    - Deprive an authorized user access to a resource;
    - Obtain or attempt to obtain extra resources beyond those allocated; or

- Circumvent security measures in order to gain access to any automated system for which proper authorization has not been granted.

- Do not download, install, or run security programs or utilities that might reveal weaknesses in the security measures or access privileges of any system. Inform the SSO when you find such a weakness.

- No user, software developer, or Web developer should write or put into production any computer code, program, or script that is considered to be a *Trojan Horse* or any *back door* means of accessing the system or applications.

- Any user that is found to introduce *Trojan Horse* type code, program, or script, is subject to prosecution under local, State, and Federal law and is subject to local department/corporate policies that enforce disciplinary action up to and including dismissal. This policy includes the use of `.rhosts` and `.netrc` files in any user's home directory for the purpose of avoiding entering keystrokes to gain access to any system.

- No user of any software application should attempt to circumvent any security measures for that application.

- Users should access only the resources of an application that are necessary to perform their job assignments, even though an application may grant further access privileges.

Trojan Horses

A Trojan horse is an application that attempts to circumvent any security measures

Unofficial use of Government equipment

- Users should be aware that personal use of information resources is not authorized unless sanctioned by management.

- Do not utilize corporate/Government resources for commercial activity or any venture related to personal profit or gain.

- Do not utilize corporate/Government resources for behaviors that are unethical or unacceptable for the work environment.

Remote access

- The project may authorize remote access to COD. It is understood that remote access poses additional security risks, but may become necessary for certain job functions.

- If remote access is allowed, the CIO and the security office will regularly review telecommunications logs and COD phone records, and conduct spot-checks to determine if COD business functions are complying with controls placed on the use of dial-in lines.

- All remote access calls will use appropriate passwords.

- Do not divulge remote access details to anyone. If an employee needs dial-up access, refer him or her to the Technical Architecture team.

Connection to the Internet

- Use of corporate/Government resources to access the Internet must be approved, and the access should be used for authorized business purposes only.
- Use of corporate/Government resources for accessing the Internet for personal gain or profit, even though you may be using your own ISP, and on your lunch hour/break, is unacceptable.
- Use of corporate/Government provided Internet access is subject to monitoring. Accessing web sites that contain material that is deemed by management to be inappropriate for the workplace, including but not limited to obscene, or sexually oriented material, is prohibited. Disciplinary action may be taken.

E-Mail

- Users will take full responsibility for messages that they transmit through corporate/Government computers and networks facilities.
- Laws and policies against fraud, harassment, obscenity, and other objectionable material apply to electronic communications as well as any other media. Corporate, local, state, and federal laws/rules and regulations may also apply.
- All e-mail that is transmitted on corporate/Government servers is subject to monitoring by corporate/Government personnel.

Copyright

- Never install or use any software that has not been specifically licensed or authorized for use.
- Never download software from the Internet to corporate/Government systems (which is strictly prohibited) without prior authorization/approval. Follow defined procedures for downloading software.
- Adhere to all purchased software copyright, duplication requirements, and license agreements that are imposed by the vendor. Violations place the individual, the corporation, and/or the Government at risk.
- Copyright licenses for software used by COD program personnel must be understood and complied with.

User IDs

- Do not share user identification (IDs) or system accounts with any individual.
- When leaving a session unattended for a short period of time, lock the keyboard with a password-protected screen saver.
- Employ the automatic password/screen saver option feature offered by the operating system (in Windows, use **SETTINGS**, **DISPLAY**, **SCREEN SAVER**) and set the time for 15 minutes as a minimum.)

- Logoff when leaving your session unattended for an extended period of time.
- Be aware of logon and logoff times to ensure that someone else is not using your ID.

Passwords

Your password SHOULD...

- Be difficult to guess (Do not use names that are easily identified with you or appear in a dictionary, to include anniversary dates, etc.)
- Be changed frequently (at least every 90 days).
- Contain a minimum of 8 characters in length.
- Contain alphabetic and numeric characters (1 special character, 4/5 alphabet, 3/2 numeric).
- Contain at least three of the four criteria: upper case, lower case, number, or special character.
- Be changed immediately if you suspect it has been compromised.

Your password SHOULD NOT…

- Have the same character/alphanumeric appear more than once.
- Be shared with anyone.
- Be written down, posted on a "yellow stickie" stuck to your monitor or computer, documented on your calendar, stored in your wallet or purse, etc.
- Be stored on a programmable key.

Do Not check the memorize password feature on your system, which would eliminate the necessity to respond to a password prompt with other than pressing the RETURN key.

Users

- Users are personnel authorized and able to access department IT assets. They include operators, administrators, and system/network maintenance personnel.
- All users are expected to understand and comply with this policy document and its requirements.
- Questions about the policy should be directed to the appropriate CSO or the DCIO/IA.

All users will report security problems or incidents to their respective SSOs or other appropriate security official as soon as practical. Violations of security policies may lead to revocation of system access or disciplinary action up to and including termination.

Privacy Act Data Protection

- Privacy Act data must not be transmitted unprotected.
- Privacy Act data includes: SSN, Name, Date of Birth, Mother's Maiden Name, and other information used to identify a specific individual.
- Documents containing privacy act data are to be password protected using that month's password when distributed electronically.
- The password is distributed monthly by the FSA SSO.
- Contact your company's COD System Security Officer if you need to be added to the distribution list for the monthly password.
- Notify your SSO if any violations of this policy occur.

Other Policies and Procedures

The Rules of Behavior are not to be used in place of existing policy, rather they are intended to enhance and further define the specific rules each user must follow while accessing the COD system. The rules are consistent with the policy and procedures described, but not limited to, the following directives:

- Freedom of Information Act.
- Privacy Act.
- Computer Security Act.
- Government Information Security Reform Act (GISRA).
- OMB publications.
- National Institute of Standards and Technology (NIST) publications.
- Network security manuals/procedures.
- System security manuals/procedures.
- Personnel security manuals/procedures.
- Software security manuals/procedures.
- Department of Education publications.

These responsibilities will be reinforced through scheduled security awareness training.

I acknowledge receipt of, understand my responsibilities, and will comply with the "Rules of Behavior" for the COD System. I understand that failure to abide by the above rules and responsibilities may lead to disciplinary action up to and including dismissal. I further understand that violation of these rules and responsibilities may be prosecutable under local, State, and/or Federal law.

Print Name _____

Signature _____

Date _____